A CERTIFICATION METHOD

The present invention relates to a certification method and system. The present invention particularly, but not exclusively, relates to public key cryptography and a process for the issuing of digital certificates to bind a person's identity to a particular public key.

The basis of public key cryptography is the generation of a public and private key pair for use in the encryption and decryption, and signing and verifying, of information transmitted over public access communication lines. Key pairs are mathematically related, but it is not practically feasible to derive a private key from its corresponding public key. A person may openly distribute the public key but the person must keep secret the private key. Anyone wishing to send information to a person encrypts the information using that person's public key. The recipient, being the sole possessor of the corresponding private key, is the only person who can decrypt that information.

For a number of electronic commerce applications, a trusted third party, known as a Certification Authority (CA), is needed to bind a person's identity or information, such as privileges, memberships, account numbers, etc., to their public key. The CA issues a digital certificate, which is essentially a form of electronic identification that binds two or more pieces of information, such as the identity of the person and a particular public key. Throughout the specification a reference to person is intended to include a reference to an organisation or individual.

The process of binding a public key to a person must be secure so that the CA can issue a digital certificate and be accordingly held responsible for it. At present, there is a weakness in certification processes used by CAs. Once the CA receives the public key generated by a person's equipment, together with other data concerning the person, a registrar of the CA contacts the person, or vice versa, to correctly identify them with reference to the person's identifying or personal data that has been provided. This is normally done by having the contacted person repeat to the registrar personal details, such as mothers' maiden names and drivers' licence numbers. This identifying information however is only related to the identifying or personal data submitted by the person and does not relate whatsoever to the public key which is used for all future communications. The public key can therefore become separated from the

person's data held by the CA or substituted and there is currently no method of relating the public key to the person other than by storing it with the person's data. It is desired to overcome this problem or at least provide a useful alternative.

The present invention provides a certification method, including:

receiving a public key of a public/private key pair generated by a system of a person;

processing said public key to generate a communicable code representative of said public key;

identifying said person, said identifying including having said person convey said communicable code; and

generating a digital certificate, said certificate including said public key.

The present invention also provides a certification system, including:

means for receiving a public key of a public/private key pair generated by a system of a person;

means for processing said public key to generate a communicable code representative of said public key; and

means for generating a digital certificate after identifying said person, said identifying including having said person convey said communicable code, and said certificate including said public key.

The present invention also provides a certification program stored on computer readable storage media, including:

code for receiving a public key of a public/private key pair generated by a system of a person;

code for processing said public key to generate a communicable code representative of said public key; and

code for generating a digital certificate after identifying said person, said identifying including having said person convey said communicable code, and said certificate including said public key.

The present invention also provides an identification process, including:

receiving a public key of a public/private key pair and identifying information of a

person;

deriving a communicable code from said public key; and

having said person convey said communicable code.

The present invention also provides an identification process, including:

generating a communicable code from a public key of a public/private key pair; and

binding said public key to identifying information of a person when said person conveys said communicable code.

A preferred embodiment of the present invention is hereinafter described, by way of example only, with reference to the accompanying drawings, in which:

Figure 1 is a block diagram of a preferred embodiment of a certification system; and

Figure 2 is a flowchart of steps executed by the system.

Referring to Figure 1, there is shown a person 20 who can interact with a telephone 42 or the person's computer system 32. The computer system 32 can communicate with a certification computer system 30 of a Certification Authority (CA), or a registrar acting for or on behalf of the CA, via a communications channel 60. A registrar 10 of the CA interacts with the certification system 30 and a telephone 40 to communicate with and confirm the identity of the person 20. The registrar 10 and the person communicate verbally over a communications channel 62 connecting the telephones 40, 42. The computer systems 30, 32 may communicate with each other independently or on instructions from the registrar 10 or person 20, respectively. The communications channels 60, 62 may be constituted by any voice or data transmission media. For example, the communications channel 60 may be a TCP/IP link.

Referring to Figure 2, a person wishing to obtain a certificate from the CA would visit the CA web site 100 using the person's computer system 32. This is the first step in the process of obtaining a certificate and is one way by which the person may perform the second step of filling out the registration form 110 and sending it to the CA over the communications channel 60. The registration form captures personal or identifying information about the person which could be used to confirm the identity of that person over the telephone. Once the person fills out and sends the registration form 110, the person is not aware of the subsequent steps in the process until he or she receives a registration ID, at step 210, in the form of a communicable

code. The intervening parts 120 to 200 of the process are conducted by the computer systems 30, 32 automatically.

The computer system 30 of the CA receives and processes the submitted registration form at step 120 and sends an instruction to generate the public/private key pair 130 to the computer system 32 of the person. The received registration information may be stored in a database at this point or may be stored once the person's public key is received and the corresponding alphanumeric code is generated together with that information. Once the computer system 32 has received the instruction to generate a public/private key pair, it generates, according to algorithms commonly used by browser applications, such as Netscape Navigator or Microsoft Internet Explorer, a public/private key pair at step 140. The private key is kept securely by the person in the memory of the computer system 32 or another data storage medium, while the public key may be used by anyone wishing to send information to the person. The person's computer system 32 sends the public key 150 to the computer system 30 of the CA. Once the computer system 30 receives the public key it generates the communicable code, at step 180. The public key is represented as a value of the Abstract Syntax Notation No. 1 (described in ASN.1 by ITU) data type SubjectPublicKeyInfo (defined in standard X.509 by ITU), encoded according to the distinguished encoding rules (DER by ITU) and passed through a secure one-way hash algorithm such as SHA-1 (defined in the U.S. Government Federal Information Processing Standard (FIPS) 180-1). The output of the hash algorithm is truncated to 40 bits and converted to 8 base-32 characters. The numerals and upper case letters (excluding '0', '1', 'O' and 'I' to avoid confusion) are used as the base-32 character set. For example, the code may be 8JQ3 UEB5. The code is communicable, to the extent that it is sensibly communicable by the person to the registrar on the communications channel 62, which may include a telephone call or facsimile message. The public key is not sensibly communicable on an identification channel 62 as it is a large mathematical quantity typically consisting of hundreds of decimal digits. The information on the person generated and received is then stored in a database, at step 190, by the CA.

The communicable alphanumeric code is sent to the person as a registration ID, at step 200. The person will probably not know that the registration ID is, in fact, derived from the public key generated by the person's computer system 32. At some time after the person receives the registration ID 210, he or she establishes telephone communication with the

registrar of the CA and provides the registrar with relevant person identification information, at step 220. The registrar confirms the relevant information 230 and requests the person to say the registration ID 240. Once the person provides the registration ID 250 to the registrar, the CA has a public key from computer system 30 and a confirmed identity and communicable code from the registrar. The CA compares, at step 260, the code to a value recalculated from the public key using the secure hash algorithm and, if they match, issues a digital certificate that lists the public key and confirmed identity 270. The digital certificate thereby incorporates the public key and the confirmed identity data and is signed by the CAs private key. The certificate may be sent, at step 280, to the person and stored, at step 290, on their hard drive, floppy disk, smart card, etc. and/or the certificate may be published in another system, such as electronic white pages.

As the alphanumeric code used in the identification process is derived directly from the public key, the CA can ensure the identification information confirmed by the registrar and the public key are bound as a pair, which ensures the digital certificate contains the correct information.

The steps of the certification process described above which are executed on the computer systems 30 and 32 are preferably executed by, or under the control of, computer programs resident on the respective systems 30 and 32. The steps may also be wholly or partly executed by dedicated hardware included in the systems, such as application specific integrated circuits (ASICs). The systems 30 and 32 may comprise single systems in one location or may comprise distributed systems with their software and hardware components in different locations.

Many modifications will be apparent to those skilled in the art without departing from the scope of the present invention as herein described. For example, the person 20 being identified may be aware that the registration ID is a summary of the public key. Their system 32 could be used to generate the alphanumeric code, which acts as a key summary, and the person can then convey the code with the identifying information which is to be bound to the public key. Also when the registrar identifies the person and has the person convey the communicable code, a number of techniques could be employed to initiate or achieve this. For example, the registrar may phone the person, the person may phone the registrar, as discussed

above, or the person can physically visit, fax or send mail to the registrar, and/or vice versa.

5